EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	EXDIR		X		
4	D/ICS		X (for SECOM)		
5	DDI				
6	DDA		X (for D/OC & D/OIT)		
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/Pers				
14	D/OLL				
15	D/PAO				
16	SA/IA				
17	AO/DCI				
18	C/IPD/OIS				
19	NIO				
20					
21					
22					
	SUSPENSE		Date		

Remarks

STAT

Executive Secretary

2 Apr 85

Date

3637 (10-81)

NTISSC
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

OFFICE OF THE EXECUTIVE SECRETARY

NTISSC 12-85
27 March 1985

Comm

MEMORANDUM FOR THE MEMBERS AND OBSERVERS, NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE (NTISSC)

SUBJECT: "National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems"

This memorandum forwards a revised copy of the subject policy which will be voted upon at the 10 May meeting of the NTISSC. The issues regarding use of satellites launched prior to or during the five-year period after the policy is effective, definition of civil satellites, and the meaning of mission data have been significantly clarified. NSA has addressed certain national security concerns, expressed below, regarding U.S. Government use of space systems.

AMSAT and COMSAT, two major satellite interests, have agreed in principle to the objectives of the policy and are in the process of incorporating cryptographic techniques presently being evaluated by the Government.

The need to protect telemetry, tracking and control (TT&C) and mission data is critical to Government or Government contractor use of U.S. civil and commercial satellites and vital to the proprietary interest of commercial users. As an example of the need to protect science mission TT&C data, the Space Telescope to be launched by the shuttle will represent more than a billion-dollar investment and a decade of development. Without the protection of TT&C data, use of relatively unsophisticated electronic intervention could result in damage to the telescope by pointing it toward the sun. Further, damage to U.S. prestige would occur should an adversary derail a planetary probe, such as Galileo on its route to Jupiter. Vandalism or intentional subversion of a space system is not so impossible as to be ignored.

The need to protect mission data becomes evident when considering that remote sensing, as by LANDSAT, and materials processing such as accomplished on Spacelab, may soon generate substantial amounts of unclassified national security-related information. It would not be in the best interest of the nation to allow potential adversaries uncontrolled use of overhead imagery; nor should the derivation or yields of space-processed semiconductors and new metal alloys be revealed unintentionally. If, as has been suggested, massive space structures which have national security value are to be built using non-terrestrial (lunar) materials, certain information from such operations should be protected. At present, these prospects are of scientific or proprietary interest only, but the situation may be quite different within the next several years.

Technology driving space exploitation is being matched by that to produce useable and effective communications protection measures. As light, low-power, easily embedded and relatively inexpensive COMSEC measures become available, opposition to including such techniques in space systems will diminish.

STAT

/ EXECUTIVE SECRETARY

Encl:
a/s

FOR OFFICIAL USE ONLY

NTISS

DRAFT

NATIONAL POLICY

ON

APPLICATION OF COMMUNICATIONS SECURITY TO U.S. CIVIL AND COMMERCIAL SPACE SYSTEMS

NATIONAL TELECOMMUNICATIONS AND
INFORMATION SYSTEMS SECURITY COMMITTEE

FOREWORD

The use of satellites for the transmission of U.S. Government and Government contractor telecommunications is expanding rapidly. The National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems was developed by the National Telecommunications and Information Systems Security Committee (NTISSC) in recognition of a need to protect U.S. space systems.

It is a policy to protect both the relayed telecommunications transmitted over space system circuits, and the telecommunications functions on civil space systems which implement critical telemetry, tracking, control (TT&C) and mission data functions. Government or Government contractor use of civil space systems for telecommunications is limited to those protected by approved techniques. The Government shall encourage the similar protection by approved means of all commercial space systems.

This policy is effective immediately, and supersedes NCSC-10, "National Policy for Protection of U.S. National Security-Related Information Transmitted Over Satellite Systems," dated 26 April 1982.

NATIONAL POLICY
ON
APPLICATION OF COMMUNICATIONS SECURITY TO U.S. CIVIL AND COMMERCIAL SPACE SYSTEMS

SECTION I - POLICY

1. Government classified and Government or Government contractor national security-related information transmitted over satellite circuits shall be protected by approved techniques from exploitation by unauthorized intercept.

2. Government or Government contractor use of U.S. civil (Government-owned but non-DoD) and commercial satellites launched five years from the date of this policy shall be limited to space systems using approved techniques necessary to protect the essential elements of telemetry, tracking and control (TT&C) and mission data (data generated onboard the satellite, as in LANDSAT). Nothing in this policy shall preclude use of satellites that do not employ TT&C protection if those satellites are launched prior to or during the specified five-year period.

SECTION II - EXCEPTIONS

3. Exceptions to this policy may be granted by the NTISSC in consultation with Federal departments and agencies, as well as the private sector; satellites intended exclusively for unclassified scientific missions may routinely be granted exceptions.

SECTION III - DEFINITIONS

4. Space systems consist of the spacecraft or satellite, command ground station, data acquisition stations, telecommunications, TT&C, and mission data functions.

5. Mission data is originated by the spacecraft to accomplish its operating objectives. Protected essential elements are those functions of TT&C which would deny unauthorized control of the space system.

SECTION IV - HEADS OF DEPARTMENTS

6. The Director, National Security Agency, in coordination with other departments or agencies as appropriate, shall assess space systems telecommunications, TT&C, and mission data functions to determine their vulnerability to unauthorized use and provide approved protection techniques and guidance.

7. Nothing in this policy shall relieve the heads of Federal departments and agencies of their authority and responsibility for executing other measures to assure the adequate protection of their telecommunications.